

Protect Your Identity



Tips and Tools for Safeguarding
Your Personal Information From
Being Used Fraudulently





What Is ID Theft?

Many people are falling victim to a new breed of criminal known as "identity thieves." These are crooks who operate in both the physical and virtual worlds, searching for opportunities to steal valuable pieces of personal information that belong to someone else.

For the identity thief, the phrase "a little goes a long way" rings true. With a minimal amount of valid information (e.g., Social Security Number, driver's license, etc.), a skilled thief can quickly assume an individual's identity to conduct numerous crimes such as:

- ✓ opening new bank accounts and writing bad checks
- ✓ establishing new credit card accounts and not paying the bills
- ✓ obtaining personal or car loans
- ✓ getting cash advances



- ✓ establishing a cellular phone or utility service and running up bills
- ✓ changing your credit card mailing address and charging on your existing accounts
- ✓ obtaining employment
- ✓ renting an apartment, then avoiding the rent payments and getting evicted

What Do Victims Face?

One of the biggest problems with cases involving identity theft is that it can take months before the victim is aware of any wrongdoing. The victim typically learns of the crime after he or she receives a collection agency letter or is turned down for a loan because of a negative credit rating. When it gets to this point, a victim will often end up spending many hours reclaiming his or her identity and straightening out financial matters.

How Thieves Steal an Identity

ID theft can occur in a number of different ways. Here are some common scenarios.

Dumpster Diving – Thieves rummage through trash cans for pieces of unshredded personal information that they can use or sell.

Mail Theft – Crooks seek out and steal from unattended/unlocked mailboxes to obtain pre-approved credit offers, bank statements, tax forms, and/or convenience checks. They also look for credit card payment envelopes left in the mailbox for postal carrier pick-up.

Inside Sources – A dishonest employee with access to personnel records, payroll information, insurance files, account numbers and/or sales records can wreak havoc.

Imposters – Many identity theft victims have been taken in by an individual who fraudulently posed as someone who had a legitimate or legal reason to access the victim's personal information (e.g., landlord, an employer, marketer, etc.).

Spyware – Cyber-thieves use a software application that can be remotely installed on your computer without you knowing. This special snoopware lets the thief access everything you do online.

Online Data – Thieves can purchase sensitive personal information about someone (e.g., name, address, phone numbers, Social Security Number, birth date, etc.) from an online broker.

Direct Access to Personal Documents in the Home –

Unfortunately, there are identity thieves who can gain legitimate access into someone's home and personal information through household work, babysitting, healthcare, friends or roommates, etc.

Purse/Wallet Theft – Stolen purses and wallets usually contain plenty of bankcards and personal identification. A thief can have a field day using this information to obtain credit under the victim's name or to sell the information to an organized-crime ring.

Phishing Scams – Thieves who appear to be trusted financial institutions use phony e-mails to hook someone into giving them your financial and personal information.

DID YOU KNOW?

The law allows all consumers to order one free credit report from each of the three nationwide credit bureaus once a year. You can order by calling 1-877-322-8228 or by visiting www.annualcreditreport.com

If You Become a Victim of Identity Theft

1 Contact one of the national credit bureaus to place a fraud alert in your file and request a free copy of your credit reports.

You need only to make a toll-free call to any one of the three credit bureaus. The other two will be automatically notified to place a fraud alert in your file and send you a credit report.

2 File a report with your local police or a law enforcement agency.

Be sure to get a report number and/or copy of the report should anyone request proof of the crime.

3 Close any accounts you know or think have been tampered with or opened fraudulently.

Contact the fraud departments of creditors (e.g., credit card issuers, phone companies, utilities, banks, other lenders, etc.). Describe your identity theft problem and follow up with a letter or affidavit. This is very important for credit card issuers, since the consumer protection law requires cardholders to submit disputes in writing.

Take advantage of the Federal Trade Commission's (FTC's) **ID Theft Affidavit** when disputing new unauthorized accounts.

It is a special tool developed to help simplify the ID theft reporting process for consumers. The ID Theft Affidavit is a standard form that can be used by victims to report the same information to different companies, such as the three major credit bureaus, and other banks or creditors where an account has been opened and/or used under the victim's name.



For a copy of the ID Theft Affidavit, visit www.consumer.gov/idtheft or call 1-877-ID-THEFT.

4 File a complaint with the FTC.

The FTC handles complaints from victims of identity theft, provides information to those victims, and refers complaints to appropriate entities, including the major credit-reporting agencies and law enforcement agencies.

FTC CONTACT DETAILS	
BY PHONE	USING ONLINE COMPLAINT FORM
Toll-free 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261	www.consumer.gov/idtheft

CREDIT BUREAU	CONTACT DETAILS
Equifax www.equifax.com	888-766-0008
Experian www.experian.com	888-397-3742
TransUnion www.transunion.com	800-680-7289

DID YOU KNOW?

Under the Federal Credit Reporting Act (FCRA), you have the right to:

- **Ask the national credit bureaus to place an initial or extended fraud alert in your file.** These alerts require that creditors contact you before opening any new accounts or changing existing accounts.
 - An **initial alert** stays on your file for at least 90 days and entitles you to a free copy of your credit report on file at each of the three credit bureaus.
 - An **extended alert** stays in your file for seven years and entitles you to two free credit reports in a 12-month period from the time the alert was placed.
- **Obtain documents relating to any fraudulent transactions made or accounts opened using your personal information.** A creditor or other business must give you copies of applications and other business records relating to transactions and accounts that resulted from the theft of your identity, but you must ask for them in writing.

FREE CONFIDENTIAL COUNSELING

If you are a victim of identity theft, you can receive free confidential counseling by calling Call for Action at 1-866-IDHOTLINE. You can also go to their website at www.callforaction.org to request assistance.

5 Take other appropriate actions, depending on your identity theft circumstances:

IF YOU SUSPECT:	DO THE FOLLOWING:
<ul style="list-style-type: none"> ✓ your mail has been stolen to obtain bank and credit card statements, bills, pre-screened credit offers, etc., or the thief has submitted a change-of-address form to redirect mail 	file a report with the U.S. Postal Inspection Service Office. Telephone numbers are listed in the white pages under federal government.
<ul style="list-style-type: none"> ✓ the thief has changed a billing address on a credit card account 	<ul style="list-style-type: none"> • contact your credit card-issuing bank to establish a password to be used before any inquiries or changes are made on the account. • close all accounts that have been tampered with; request new PINs and passwords.
<ul style="list-style-type: none"> ✓ your Social Security Number has been stolen 	contact the nearest Social Security Administration office to report the suspected abuse.
<ul style="list-style-type: none"> ✓ you have lost your passport or believe it has been stolen or used fraudulently 	contact the local United States Department of State (USDS) field office listed in your telephone directory.
<ul style="list-style-type: none"> ✓ the thief has used your personal information and/or Social Security Numbers to get a driver's license (or non-driver's license ID) 	notify your state Department of Motor Vehicles (DMV).

Phishing Scams . . . Don't Get Lured In

"Phishing" is an e-mail scam involving fraudsters who pretend to be a legitimate business such as a financial institution, credit card company, online service provider, or retailer, etc. Hiding behind the anonymity of the Internet, they send out "official-looking" e-mails to trick you into divulging your account numbers, passwords, Social Security Numbers, and other sensitive data. In most cases, the e-mail claims there is an account problem or warns of a possible account fraud threat. Either way—the whole idea is to convince you there is an immediate need to update your financial or personal information.

- ✓ **Treat unsolicited e-mail requests for financial information or other personal data with suspicion.** Do not reply to the unsolicited e-mail or respond by clicking on a link within the unsolicited e-mail message.
- ✓ **Contact the actual business that supposedly sent the e-mail to verify if it is genuine.** Visit a web site or call a phone number that you know to be legitimate.
- ✓ **Look for the lock.** Prior to entering account information on any web site, be sure to look for the "locked padlock" in the browser or "https" at the beginning of the web site address to make sure the site is secure.



Many financial institutions use e-mail to communicate with customers and direct them to their sites, where the customers may be asked to enter personal information as part of registering for a service. No legitimate financial institution will send an e-mail to you for the sole purpose of asking you to give them account details. They already have this information.

- ✓ **Forward any suspicious e-mails claiming to be from Visa or your Visa card issuer to phishing@visa.com.** You can also send any suspicious e-mails to the Better Business Bureau at nophishing@bbb.org and immediately call your issuing financial institution.

Visa Layers of Security for Cardholders



No single solution is sufficient when it comes to stopping fraud and identity theft. That's why Visa® has put into place a security program that provides multiple layers of protection to help cardholders shop anywhere, anytime, any place with greater comfort and confidence.

It all adds up “layer by layer” through initiatives such as these:

Zero Liability

Visa offers consumers zero liability* fraud protection for unauthorized transactions. If you discover unauthorized Visa credit or check card charges under your name, your liability is \$0—you pay nothing.

*U.S.-issued only. The zero liability policy does not apply to commercial card or ATM transactions, or to PIN transactions not processed by Visa. See your Cardholder Agreement for more details.

Under the Fair Credit Billing Act, consumer liability for unauthorized credit cards is limited; in most cases, to \$50 per card.

ID Theft Assistance

In recognizing the importance of taking the “hassle factor” out of being an identity theft victim, Visa has launched a special program in partnership with Call for Action (www.callforaction.org) to help victims recover in the event of identify theft. Victims can now receive free, confidential assistance from trained identify theft counselors by calling 1-866-ID-HOTLINE.

Verified by Visa

Visa was the first to launch new technology that required a personal password for Internet purchases to confirm the identity of the cardholder. Verified by Visa helps secure online purchases at participating merchants by authenticating cardholders' identities during online transactions.

Three-Digit Security Code

Another layer of fraud prevention resides with the use of Visa's Card Verification Value 2 (CVV2), the three-digit code on the back of all credit and debit cards. CVV2 helps online and phone merchants confirm that the customer is in possession of the actual card.

Continuous Monitoring for Fraud

Visa is continually monitoring its payment systems to detect unusual spending activity and issue real-time alerts to banks, who, in turn, then call their cardholders to confirm transactions.

Anti-Phishing Technology

Visa has also joined the Phish Report Network (www.phishreport.net), a database which allows financial institutions and other companies to report their legitimate and fraudulent web sites so that e-mail providers and others can block the e-mails from consumers' in-boxes.

Anti-Fraud Consumer Education

Visa provides extensive consumer education on fraud topics such as phishing and identity theft at www.visa.com/security.

To Find Out More

The Internet is full of web sites offering helpful advice on ID theft. To access publications on the subject and find out more about what you can do to protect yourself, check out these sites:



Call for Action	www.callforaction.org
Federal Trade Commission	www.consumer.gov/idtheft
Identity Theft Resource Center	www.idtheftcenter.org
Social Security Administration	www.ssa.gov
U.S. Postal Inspection Service	www.usps.gov/postalinspectors
Department of Justice	www.usdoj.gov
Phish Report Network	www.phishreport.net
Better Business Bureau	www.bbb.org
Visa	www.visa.com



Protect Yourself Against ID Theft

Here are some practical steps you can take to safeguard your personal information and reduce the rate of identity theft.

In the Home

- ✓ Shred all personal and financial information (e.g., bank statements, credit/ATM receipts, credit card offers, credit card bills, etc.) before you throw it away.
- ✓ Keep your personal (e.g., Social Security card, birth certificate, etc.) and bank/credit card records in a secure place.
- ✓ Don't give your Social Security Number, credit card number, or any bank account details over the phone unless you have initiated the call and know the business that you are dealing with is reputable.

In the Workplace

- ✓ Keep your purse or wallet in a safe place.
- ✓ Keep forms and documents with sensitive personal information in a locked drawer.

When Handling Mail

- ✓ Promptly remove incoming mail from your mailbox. Install a locking mailbox if mail theft is a big problem in your community.
- ✓ Don't leave envelopes containing your credit card payments or checks in your home mailbox for postal carrier pickup.
- ✓ Call the post office immediately if you are not receiving your mail. Some crooks are able to forge your signature and have your mail forwarded elsewhere for the purpose of obtaining information that will allow them to apply for credit in your name.

As You Go About Your Business

- ✓ If your Social Security Number is being used for identification purposes (e.g., health insurance, doctor's office), request another method of identification.
- ✓ Memorize your Social Security Numbers and/or passwords. Don't record them on paper and store them in your wallet or purse.
- ✓ Limit the number of credit cards and other personal information that you carry in your wallet or purse.
- ✓ Don't leave receipts containing your full account number at ATMS, bank counters, or unattended gasoline pumps.
- ✓ Obtain a copy of your credit report from the three major credit reporting agencies annually and review to make sure no one else is using your identity.

- ✓ Check your monthly statements to verify all transactions. Notify your bank immediately of any erroneous or suspicious transactions.
- ✓ Follow up with creditors if bills do not arrive on time. A missing bill could mean that a thief has stolen your bill, taken over your account, and changed your billing address.

When Using Credit Cards

- ✓ Report lost or stolen credit cards immediately.
- ✓ Cancel all inactive credit card accounts. Even though you do not use them, those accounts appear on your credit report, which can be used by thieves.
- ✓ If you have applied for a credit card and have not received the card in a timely manner, immediately notify the financial institution involved.
- ✓ Closely monitor the expiration dates on your credit cards. Contact the credit issuer if the replacement card is not received prior to the expiration date on your credit card.
- ✓ Sign all new credit cards upon receipt.
- ✓ Be aware of others nearby when entering your Personal Identification Number (PIN) at an ATM.
- ✓ Use passwords on your credit cards, bank accounts, and phone cards. (Avoid using the standard mother's maiden name, birth date, and the last four digits of your Social Security or phone number.)
- ✓ Take advantage of electronic bank statements if available. By eliminating paper statements, you can reduce the risk of mail and/or trash-related theft.
- ✓ Match your credit card receipts against monthly bills to make sure there are no unauthorized charges.
- ✓ If your account information is available to you through your financial institution's web site, monitor your transaction details and activity on a regular basis.

While On the Computer

- ✓ Don't disclose bank account numbers, credit card account numbers, or personal financial data on any web site or online service location unless you are absolutely sure the business you are dealing with is legitimate.
- ✓ Use anti-spyware and anti-virus software and update regularly.

